知財管理システムroot ipクラウド

ログインアカウント管理のベストプラクティス

株式会社root ip

INDEX

1. これまでのログイン管理と課題

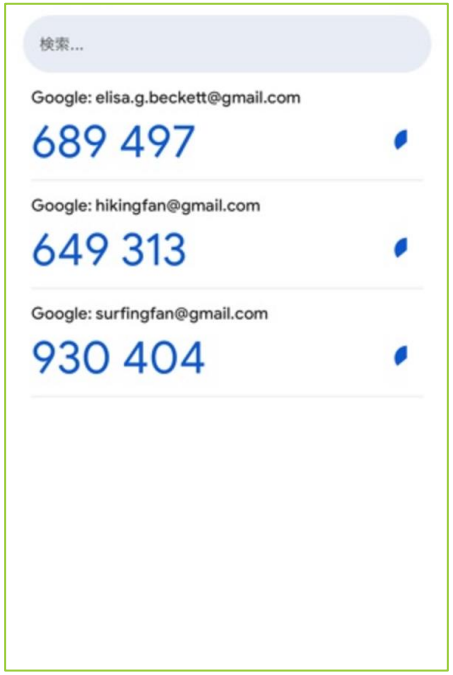
1．これまでのログイン管理と課題

パスワードログイン

シングルサインオン

IPアドレス制限

ワンタイムパスワード



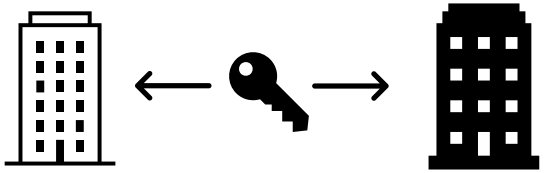
電子証明書

1．これまでのログイン管理と課題

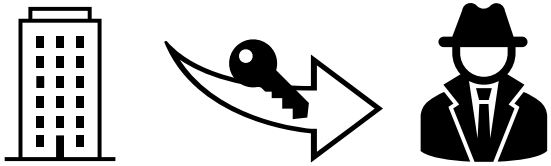
パスワードによるログインの課題

失念

流用



漏洩



> “
>
> オージス総研は2019年1月、ファイル転送サービス「宅ふぁいる便」を停止した。利用者のメールアドレスとパスワードが平文のまま約480万件流出した。暗号化やハッシュ化の必要性は認識していたものの、他の対策を優先し怠った。

引用：日経XTECH
https://xtech.nikkei.com/atcl/nxt/mag/nc/18/020600011/022600026/

あいうえお ⟶ 9f86d081884c7d659a2fea

平文　　暗号

パスワード管理はリスク大

1．これまでのログイン管理と課題

設定展開の課題

シングルサインオン

OIDC: OpenID Connect 方式（↔ SAML方式）
お客様毎にお手元で設定 → すべてのお客様が設定を行う必要あり

IPアドレス制限

ご依頼いただき弊社で設定 → 設定の変更や検証が困難

ワンタイムパスワード

強制化の仕組みなし → 勝手に無効化された場合の検知不可

電子証明書

端末毎の設定が必須 → すべての操作端末で設定を行う必要あり

複数ユーザに設定を展開することが困難

2. これからのログイン管理

2. これからのログイン管理

設定 > 基本設定 > セキュリティ設定

※ 全権ユーザ / システム管理ユーザのみ表示可能

2. これからのログイン管理

SAMLログイン設定

SAML方式によるシングルサインオンの構成（↔ OIDC）

パスワードログイン設定（★）

パスワードログインの許可・禁止の切り替え　※SAMLログインの構成が必要
従来のOIDCのシングルサインオン設定では不可

電子証明書設定（★）

電子証明書の必須・不要の切り替え

ワンタイムパスワード設定（★）

ワンタイムパスワードの必須・任意の切り替え

IPアドレス制限設定（★）

許可IPアドレスリストの編集と有効・無効の切り替え

柔軟な設定が可能に

ただし★ のうちどれかひとつ制限が必要

初期設定では電子証明書設定が必須

2. これからのログイン管理

パスワードログイン

禁止が可能

~~→失念、流用、漏洩のリスク~~

パスワード管理のリスク回避が可能

シングルサインオン

SAML方式の構成が可能

~~→すべてのお客様が設定を行う必要あり~~

管理者が構成したSAML設定で全ユーザがログイン可能

IPアドレス制限

お客様のお手元で追加変更可能

~~→設定の変更や検証が困難~~

即時の設定変更・テスト環境での検証が可能

ワンタイムパスワード

強制化が可能

~~→勝手に無効化された場合の検知不可~~

設定の強制が可能 未設定の場合はログイン不可

※ 端末にインストールする性質上、ユーザ個別の設定は必要
ログイン時にメールによる自己設定が可能

電子証明書

不要化が可能

~~→すべての操作端末で設定を行う必要あり~~

毎年の電子証明書の展開なしでのログインが可能

2. これからのログイン管理

設定 > 基本設定 > セキュリティ設定

シンプルな設定

テスト環境と独立

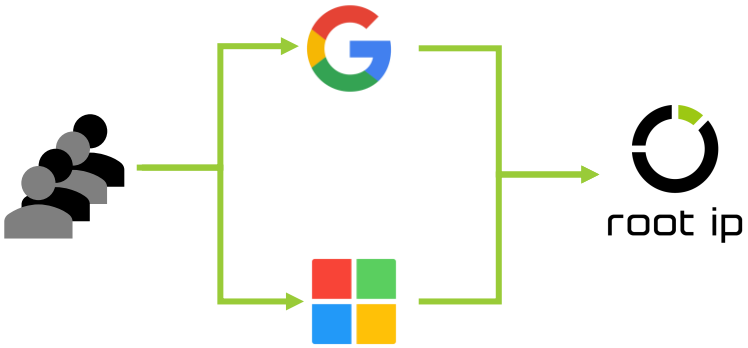
テスト環境でお試し

3. SAML設定

3. SAML設定

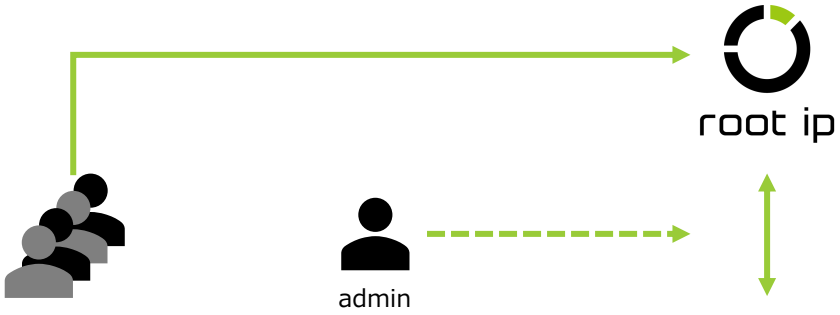
OIDC と SAML の違い

OIDC



- 各ユーザが個別に認可を与える
- 連携先は root ip が指定した Google / Microsoft のみ

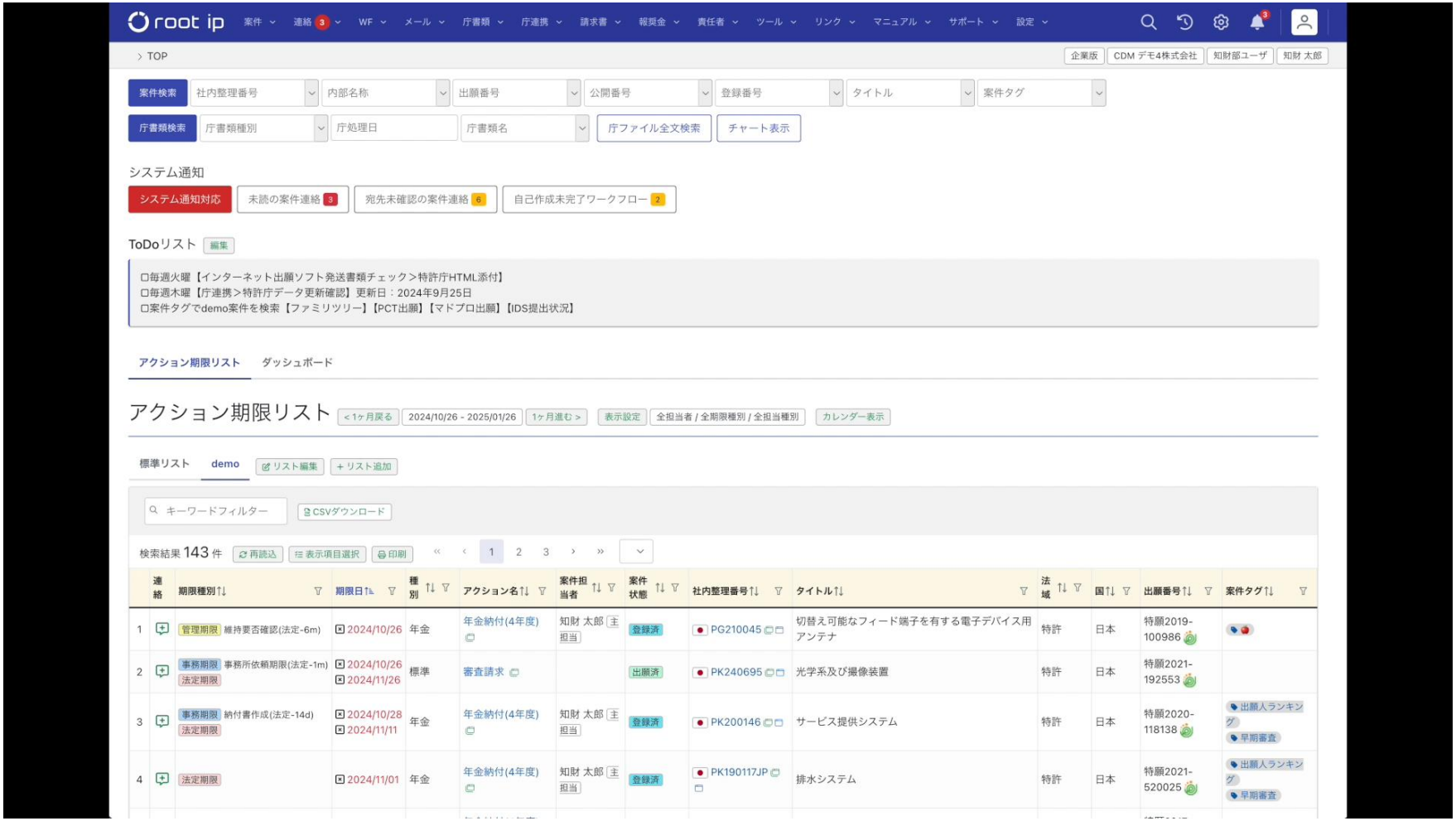
SAML



- 管理者は事前に root ip と連携先の情報交換を設定しておく
- 各ユーザは個別の設定なしでログインできる
- 管理者がログイン可能なユーザを指定できる
- SAML2.0準拠の IdP (Id Provider) ならどこでも連携可

3. SAML設定

設定実演： Microsoft Azure



3. SAML設定

ログインできるアカウント

root ip クラウドにユーザ登録があるアカウント

taro@rootip.co.jp → root ip taro@rootip.co.jp

hanako@rootip.co.jp ⇢ ログイン不可 ⇢ root ip

IdP ID – ユーザ紐付け設定

taro@rootip.co.jp　同一IDは紐付け設定不要　root ip taro@rootip.co.jp

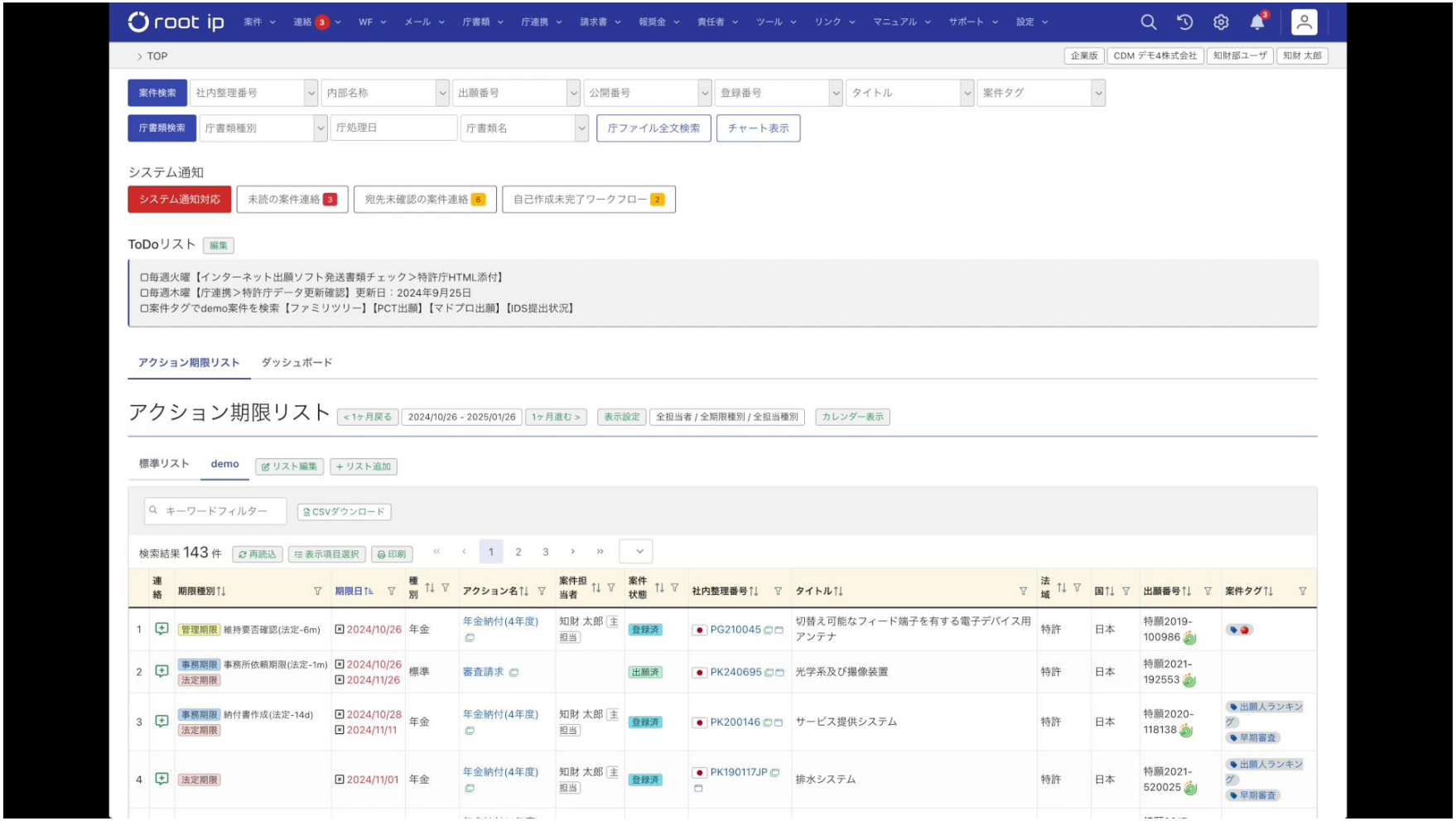
jiro@rootip.co.jp → 紐付け設定 → root ip kacho@rootip.co.jp

SAMLユーザ設定 編集 ログ

IdP側ID	ユーザ
jiro@rootip.co.jp	知財 課長

3. SAML設定

設定実演： Google Workspace



4. おすすめのセキュリティ設定

4. おすすめのセキュリティ設定

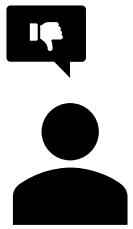
セキュリティと利便性のトレードオフ

電子証明書は不要にしちゃっていいの？

ワンタイムパスワードは必須にしなきゃダメ？

セキュリティ

利便性



多層で防御すればするほど安全（そして面倒）

お客様が面倒なことは攻撃者も面倒

4. おすすめのセキュリティ設定

おすすめ設定

事務所　知財部メインの企業

SAML/パスワード禁止 + ワンタイムパスワード必須

発明者がいる企業

SAML/パスワード禁止 + IP制限

4. おすすめのセキュリティ設定

おすすめ設定

事務所　知財部メインの企業

SAML/パスワード禁止 + ワンタイムパスワード必須

+ IP制限 + 電子証明書

発明者がいる企業

SAML/パスワード禁止 + IP制限

+ 電子証明書
(Microsoft Intune Certificate Connector)

5. 今後の展望

5. 今後の展望

ユーザ別 グループ別設定

IPアドレス制限 → 現時点でユーザ毎に設定の上書き・無効化が可能

ワンタイムパスワード

パスワードログイン禁止

電子証明書 → 同様にユーザ毎に設定の上書き・無効化を可能にする

設定のグループ化 → 知財部グループ・管理者グループなど

5. 今後の展望

SAML JIT プロビジョニング

hanako@rootip.co.jp

ログイン不可

root ip

root ip クラウドにユーザ登録がないアカウントをSAMLログイン時にその場で作成する
企業版 発明者ユーザ限定

人事データとの連携

SCIM

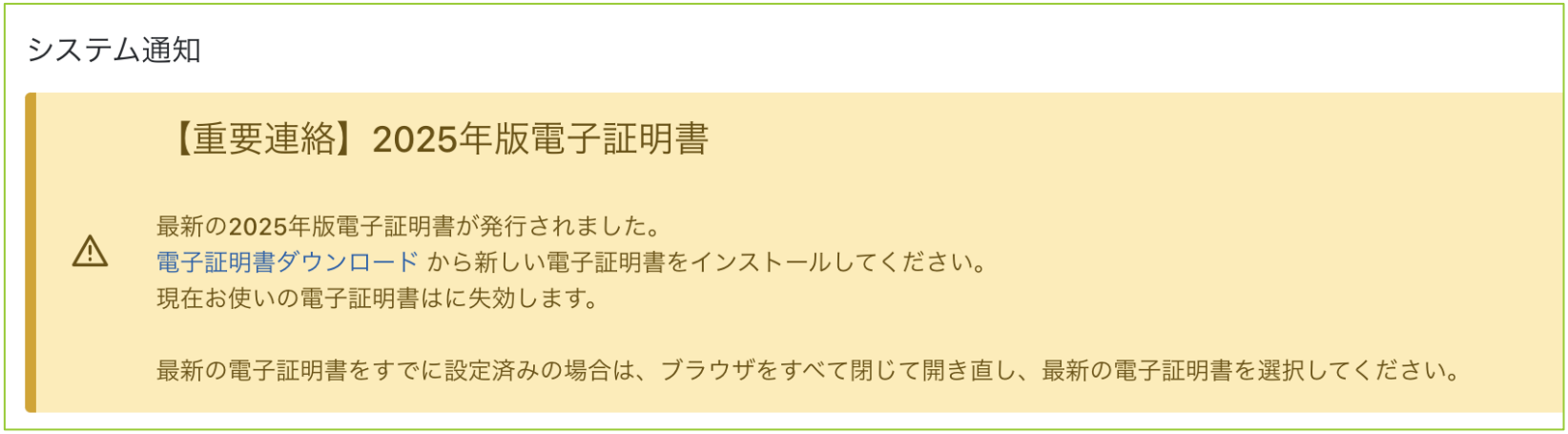
組織のユーザ・グループの情報を IdP と root ip 間で自動でやり取り
ご要望をうかがい実装を検討

バッチ実行カスタマイズ

人事データ（CSV, JSON, API）の日毎同期など

5. 今後の展望

2025年版 電子証明書



2024/12/02 から配信開始

電子証明書が不要設定になっている場合はお知らせ非表示

管理者は念のためダウンロードをおすすめ
(2024/12/02以降　設定 > 電子証明書ダウンロード)

質疑応答

root ip